Placing computer security at the heart of learning

Research Paper

Placing computer security at the heart of learning

Mike RICHARDS[1], Blaine A. PRICE[2], and Bashar NUSEIBEH[3]
[1,2,3]*The Open University*

ABSTRACT

In this paper we present the approach adopted at the UK's Open University for teaching computer security to large numbers of students at a distance through supported open learning. We discuss how the production of learning materials at the university has had to change to reflect the ever-increasing rate of technological, legislative and social change within the computing discipline, and how the university has had to rethink the role of the academic in the course development process. We argue that computer security is best taught starting at the earliest level of undergraduate teaching and continuing through in-depth postgraduate study. We discuss our approach which combines the traditional technical aspects of security with discussions on the professional and ethical issues surrounding security and privacy. This approach presents computer security and privacy in the light of relevant legislative and regulatory regimes, thus the students have a firm grounding in the relevant national and international laws. We discuss the importance of international standards for information security risk assessment and management and as well as the relevance of forensic computing to a computer security curriculum. We conclude with an examination of our course development methodology and argue for a practitioner-led approach to teaching.

KEYWORDS

Computer security, computer forensics, computer science education, informatics education, distance teaching

1 Introduction

Computer security is often given little emphasis in Computer Science teaching. It sometimes appears as an adjunct to a software engineering course or in specialist postgraduate courses. It is conspicuously absent from the Software Engineering Body of Knowledge [1] although the most recent ACM curricula recommendations [2] show both security and ethics as having mandatory courses in all of the computing and software engineering disciplines. Indeed, a US-based analysis of computing security curricula [6] argues convincingly for wide ranging teaching of security across the undergraduate curriculum. Recent high profile security failures in the UK suggest that even the general public is endorsing greater attention to security. For example, the MTAS doctor recruitment system allowed any Internet user to view personal information about some 32,000 applicants including the addresses, home phone numbers, religion and even sexuality of thousands of medical students. A security fault in a tax office allowed the financial details of every parent in the UK to be 'lost' on CDs. Other projects, including the proposed National Identity Register, the National Health Service's medical records system, and the planned UK road pricing system have all been heavily criticized by security experts as being unduly intrusive and insecure.

In December 2006, the British government's Office of Science and Innovation released an overview [7] of key trends in the areas of science and technology between 2015 and 2020. The seventh of eight so-called 'clusters' was devoted to aspects of security.

A large proportion of the cluster was devoted to the

Received ●● ●●, ●●; Revised ●● ●●, ●●; Accepted ●● ●●, ●●.

DOI: 10.2201/NiiPi.2008.5.1

currently-fashionable topic of counter-terrorism, but the report was concerned with the wider security industry. It listed a number of barriers to greater adoption of security techniques, including:

- *Increased concerns over privacy, security and trust. These will place an even greater importance on the development of effective systems of governance and of market structure. Increased unauthorised use of personal data, identification theft and other forms of fraud.*
- *Lack of public understanding and consequently support if information on and the opportunity for debate on the use of some technologies and their applications is not undertaken.*

We believe that this analysis is very relevant to the teaching of computer security, and thus places public understanding of security high on our curriculum agenda. It is clear that our ethical duty as computer scientists is to ensure that current and future practitioners are aware of the important role of security in establishing dependable computing systems. At the Open University (OU) our mission statement also requires us to be open in our admission of students and therefore to teach as many as possible at a distance. In this paper, we discuss how the OU is transforming its curriculum to embrace this entire security philosophy.

The Open University (OU) is the largest higher education institution in the United Kingdom; more than two million people have studied with the OU since it was formed in 1970. Currently, there are some 150,000 undergraduate and 22,000 postgraduate students studying with the OU from around the world as well as some 9,000 pre-university students and a further 13,000 students studying OU-validated courses at other institutions.

2 Teaching at the open university

Unlike many conventional universities, the OU only offers distance learning courses. In contrast to some American definitions of distance education (e.g., [8]) where the instructor's oral lectures are broadcast to the students, the OU develops material internally that is specifically designed for students who study asynchronously at a distance. Many conventional universities now take conventional teaching material and adapt it for the web, but OU teaching material has always been written specifically for study at a distance and to optimize the use of available technology. Through *supported* open distance learning, students are not left alone with the teaching material: more than 7,000 Associate Lecturers (ALs) support students directly by telephone, e-mail, wiki, online forum, and 'face to face' tutorials.

Almost all OU students are online with approximately 300 courses using e-learning technology to a greater or lesser extent. Online activities include electronic discussion boards, shared forums, wikis, podcasting and an electronic assignment submission system. Individual courses have annual populations that range from a few hundred students to several thousand; this allows the university to make a large investment in high quality courses and amortize the cost over many students for many years.

2.1 Traditional course development

The traditional OU course or module development methods have involved gathering a team of academics, technical support staff, and specialists such as editors, graphical designers, and software developers, who work on the production of custom course texts, software, multimedia material and assessment. In some courses this has involved building custom software development environments [3] or simulations. [4] These methods have proved successful over more than 30 years in teaching very large numbers of students at a distance: a very large investment is made in the production of a course (some introductory courses cost more than GBP 1 Million to produce) and the cost is amortized over many students over many years. The development time for such courses is between 2 and 3 years, which raises particular problems in a fast evolving subject such as computing where the cost cannot be amortized over a long period.

Once completed, a course's lifetime can be as long as ten years. Courses are revised during their lifetime, but the expense of reprinting non-digital materials is such that rewrites cannot occur more often than every 2-4 years. This presents special problems for teaching computing in general and security in particular.

2.2 Responsive course development

It is clear that relatively slow moving disciplines such as history, philosophy, or mathematics can cope with the traditional methodology more readily than a subject such as computing; but it is wholly inadequate for certain specialist areas such as computer security which are driven by fast moving developments in technology, society, and legislation. Quinn et al. [5] describe the OU Software Engineering curriculum in detail, including some course development methods. Here we describe two different methods to address the problem of timeliness in developing teaching materials

For our postgraduate Information Security Management course we used a relatively simple method of increasing the rate of course development by wrapping Open University teaching materials and assess-

ment around a published book based on an international standards document. This allowed us to use a small academic team who concentrated on developing teaching material that would support the concepts contained within the book.

The shortcoming of this approach is that it relies on the availability of suitable reference material, which may not always exist in emerging topics. An example of this problem can be found in the emerging area of forensic computing which is only now starting to appear in standard computing texts and curricula. With computing technology being involved in every aspect of business life, it is clear that the importance of forensic computing to employers and to law enforcement will continue to increase into the foreseeable future. The OU foresees a growing market for trained forensic analysts and has to include the topic within our curriculum. A new model of course development is being employed emphasizing professional expertise, relevance, and speed. Rather than relying purely on academic skills, we are building course teams around external experts and practitioners, producing directly relevant and timely courses well suited to the market.

The forensic computing course is being developed with substantial input from practitioners. The course teams comprise an external author who is an active practitioner regularly giving expert testimony in cases of terrorism, murder, conspiracy, and corporate espionage. A second industry practitioner has been employed to produce assessment materials including scenarios and realistic forensic materials. The course team additionally consists of an academic who is responsible for academic editing and coordinating the external practitioners, a course manager who coordinates with the wider university systems, and a publishing editor who guarantees quality.

Producing distance teaching material that is *both* high quality *and* up-to-date is clearly a challenge. Although these responsive methods are proving successful when compared with previous methods, we are constantly exploring new ways of improving quality without sacrificing speed of delivery as we discuss in the penultimate section. In the next sections we describe how security fits into our curriculum.

3 An early introduction to computer security

Our entry-level undergraduate course is called *Data, Computing and Information* (M150) and it covers a large number of subjects including the development of the modern networked computer, programming and the transformation of data into useful information. The course has proved to be immensely successful, attracting approximately 4,000 students each year; most of whom are new to the OU and to computing.

M150 was designed to teach a large amount of 'foundation' material — basic concepts that are unlikely to change within the lifetime of the course. Therefore, the course is dominated by very high-quality printed material whose high costs are defrayed by large print runs and obvious appeal to novice students.

A considerable part of M150 is devoted to a discussion of security and privacy. Issues of security and privacy are raised throughout the course, especially where students may be learning about the acquisition, processing and storage of personal or financial information. These two topics are explored in great detail in a pair of course units (sections); each taking approximately two weeks to study.

'*Hiding data*: *an introduction to security*' is designed as a primer to a large number of security issues. Students are first introduced to a number of real-world cases where individual or corporate privacy or security have been compromised; including examples of identity theft, financial fraud and hacking.

Students then explore how computer professionals attempt to protect information. Encryption is explored from its historical origins through to the modern era, with particular emphasis on the race between code makers and code breakers. During this part of the course, students use a web-based environment to experiment with a number of code breaking techniques where they break historical codes including homophonic ciphers and the once-impregnable Vigenère Cipher (Fig. 1).

The section of the course concludes with a discussion of the limitations of encryption and how data can be compromised through social engineering. Students will realise that security is not solely a technological issue, but one with a great number of human factors.

These factors are explored in greater detail in the following section; '*Too Many Secrets*'; which is concerned with the social and ethical issues raised in securing information. The unit considers the tensions between freedom of expression and the free exchange of ideas and the need of society to restrict such rights. Students are shown the consequences of unrestricted information exchange in the form of surveillance and piracy and then explore the various techniques used to keep information private; such as digital rights management and intellectual property legislation.

This unit has proved to be a valuable tool in assessing students; the subject is open-ended and changing very rapidly under technological and legislative pressures and has allowed the course team to set assessment on contemporary issues including music downloads, RFID and the proposed UK biometric identity cards. Students are asked to gather information about the topic and lay

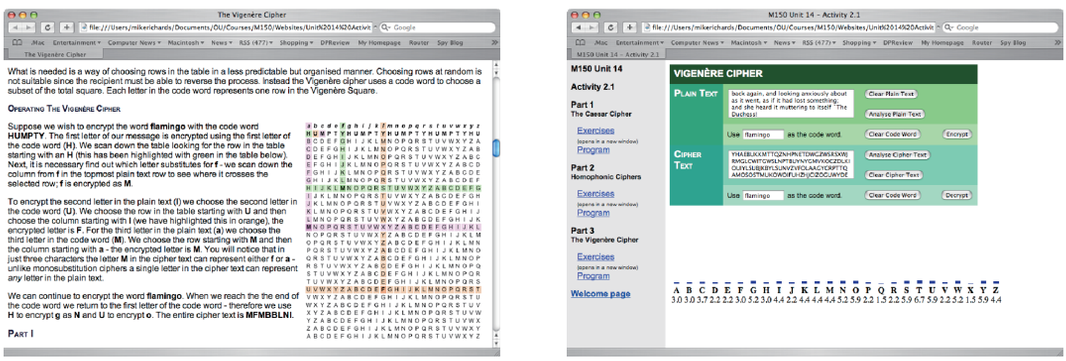


Fig. 1 M150 students exploring the Vigenère cipher. At the left, the student is introduced to the working of the cipher, at right they use a simulator to replicate Charles Babbage's original code-breaking technique.

out arguments for and against the subject, then to give their own opinion. Students are assessed not only on the technical content of their answers, but also their use of referenced sources from the Internet or libraries, and also the manner in which they express their opinions.

We have observed that the majority of M150 students express strong, coherent opinions about these subjects which they do not regard as abstract concepts, but as matters of direct concern to their everyday lives. M150 students are not studying a subject in isolation; rather they are using knowledge garnered from the course to make judgements about much larger issues.

Our experience has shown that the basics of privacy and security, including ethical and legislative issues, can be taught to inexperienced students and that they prove to be exciting subjects capable of engaging students whose interests lie beyond the scope of traditional computer science. It has also shown us that there is a clear demand for further undergraduate courses in the fields of privacy and security in later years of study.

Ironically, it is these two units that expose the weaknesses of the traditional OU course model. Although the course has been presented openly for a few years, many of the concepts discussed in these units have been superseded by technological, commercial, and legislative developments. As a consequence, the course is currently undergoing an expensive rewrite to bring the units up to date.

4 Postgraduate computer security

Although we have considerable demand for computer security teaching at undergraduate level, our current focus is on postgraduate computing courses with some input from the undergraduate law curriculum. All of our courses include coverage of relevant professional issues, many of which relate to computer security and privacy. We now discuss the contributions of two security-specific courses to our computing curriculum: Information Security Management (M886) and Forensic Computing & Investigations (M889). These courses form an introduction to the subjects and based on the results of our evaluations (see section 5) we plan to introduce a postgraduate certificate, diploma, and specialist MSc in security and IT Law.

4.1 M886: Information security management

This course focuses on developing the student's ability to analyze information security risks to an organization. It was developed in recognition of the fact that the protection of information assets underpins the commercial viability and profitability of all enterprises and the effectiveness of public sector organisations. M886 provides an overview of information security and a detailed, practical understanding of selected aspects, including IT governance and information security risk analysis and management.

M886 uses a practice-based approach where students investigate security management inside a familiar organisation (such as their employer). The teaching is geared to provide the knowledge, understanding and analysis needed to develop a practical information security management system, based on standards set by the British standards BS ISO/IEC 17799:2000 & BS 7799.

M886 is divided into three sections:

1. *An introduction to information security*—this unit discusses the current requirements on, and incentives for organisations to implement information security. Students then progress on to the process of identifying and valuing information as an organisational asset. The protection of information assets is the subject of the British standards, around which the course is based. This unit outlines the processes that must be gone through to

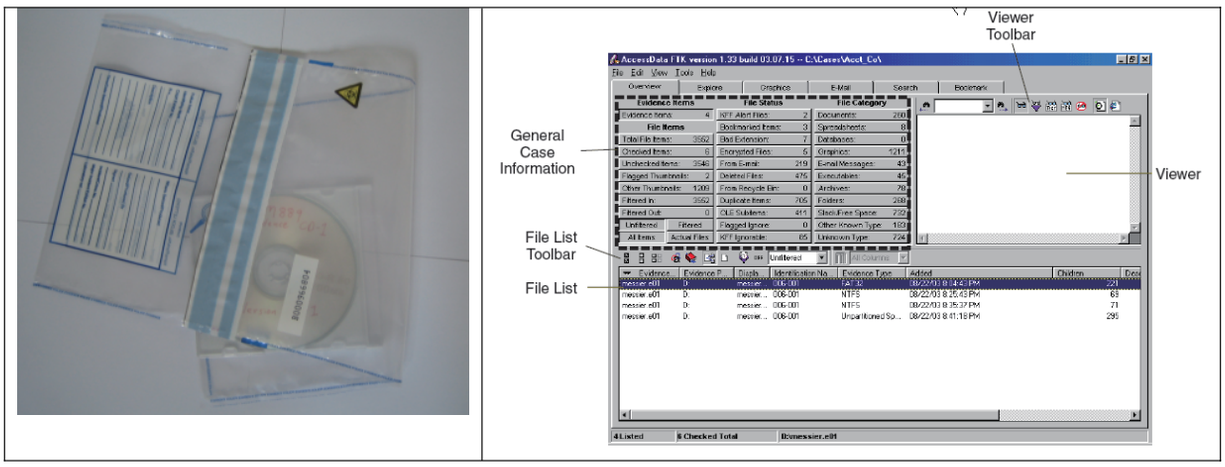


Fig. 2 Left: image of CD in official evidence bag as delivered to students, Right: screen image of Access Data Forensic Toolkit as used by students for assessment.

satisfy the requirements of the standards.

2. *Information security risk assessment*—This unit places in context the issues involved in information security risk assessment, as required by the standard. Students examine the risks that may arise in all relevant aspects of an organisation's operations, including human factors, ecommerce, web-services, and systems development. They learn how to conduct a systematic risk assessment that leads to a prioritised list of information security risks for an organisation, and the requirements for their treatment. The unit concludes with an exercise during which students conduct a risk assessment for a chosen organisation, using information contained within the British standards and the set book.
3. *Information security risk management*—by the end of this unit, the student will have completed the development of a fit-for-purpose information security management system through the management of information security risks. They will have learned to be systematic in the choice of controls that treat specific risks, and how to document their systems in accordance with British standards. There is a full discussion of the technologies that underpin the standard's controls, and the unit finishes by considering the topic of planning for when things do go wrong.

The remainder of the course requires students to conduct a piece of independent research into an issue in information security management for a real organization, analysing and evaluating the results of their research for presentation in the final examination.

4.2 M889: Computer forensics and investigations

Our most recent course, Forensic Computing and Investigations (M889), is unique in our curriculum in that it addresses professional and legal issues in depth in addition to the technical curriculum. Several weeks of study are devoted to understanding the role of the forensic computing investigator, what evidence is admissible in both civil and criminal proceedings, and which laws protect the privacy of individuals. After 8 weeks of study, the student should have a thorough understanding of which British, European or International laws govern how they may perform an investigation as well as knowing whether or not a matter is for the civil or criminal courts. Students should understand where their duties lie as both computer security professionals and as responsible citizens.

Most of the remaining weeks of study are devoted to the technical aspects of various forms of forensic computing investigations, including live and dead disk forensics as well as Internet and network forensics. Students learn the basics of media recovery and disk imaging, what kind of forensic artifacts are left behind by e-mail, web browsing and normal computer use. We introduce students to the basic features of a professional disk image analysis package. Then we present them with an evidence bag containing a CD and a set of instructions from a "customer" who suspects an employee of wrong-doing. Students then follow the forensically sound procedures they have been taught to analyze the data and produce a report suitable for management and legal briefing. Figure 2 shows examples of the evidence and the analysis program.

This course concludes with two important topics: an introduction to forensic computing research method-

ologies (including current literature on the subject) and the development of a Forensic Readiness Program for an organization. The goals here are to ensure that students are able to keep themselves up to date by finding and analyzing the relevant literature. More importantly, they should be able to analyze a new proposed methodology and discuss whether or not it is valid or applicable for a given situation. By developing and analyzing a Forensic Readiness Program for a real organization, the student is able to demonstrate practical skills in a real-world setting, as opposed to the artificial assessments often set for students.

The over-arching theme of both of our postgraduate security courses is that material is practitioner-led and related to the real-world as much as possible. Although we do make use of case studies in our teaching, our assessment emphasizes the application of techniques to real businesses and organizations in order ensure that students are able to transfer their learning beyond the academic realm.

5 Evaluation

Quality control has helped ensure that the OU has been rated the top UK university for student satisfaction [9] for each of the last three years. All teaching and evaluation materials are internally assessed by academic members of staff at all stages of preparation. Course materials can also be passed to 'developmental testers' during the development process; these are representative members of the student community who are able to provide feedback on the clarity and use of language as well as the difficulty of the material.

An academic external to the OU is a member of each course team and reviews all teaching and assessment materials as well as sitting on the 'award board' which actually issues the final student grades. The external academic is expected to write a review of the course for each presentation, listing any concerns they might have with the course. These issues must be addressed by the course team as part of their duties.

Finally, the OU's Institute for Educational Technology (IET) poll students at the end of courses. These are detailed surveys covering every aspect of the course including quality of materials, tuition, difficulty and the general student experience. More specific surveys are conducted on new courses with the intention of identifying specific problems with novel materials or teaching methods. Students can complete either a printed survey or complete the poll over the Internet with some 60% of students returning some or all of their survey. The aggregated results of the survey are presented to course teams with the intention that any necessary changes can be made - either when materials are reprinted, or by providing additional teaching materials to the associate lecturers.

6 New developments in teaching

In this section we look at innovations currently under way (but not yet evaluated) for improving the teaching of these subjects and sharing teaching experience and materials among institutions.

6.1 OpenLearn: Open source courses and teaching tools

Part of the mission statement of the Open University is to promote both educational opportunity and social justice worldwide. One aspect of this is OpenLearn (www.open.ac.uk/openlearn), a two-part $10 million open content project. The LearningSpace part of OpenLearn aims to make more than 5400 hours of OU high quality learning curriculum freely available worldwide for anyone to study or re-use. The LabSpace is a virtual area that encourages a community of practise to develop around the sharing and re-using of the resources found in the LearningSpace. Educational and professional practitioners and more adventurous learners can download materials, reversion them for their own purposes and upload the amended materials to the Labspace. Following a formal peer review these could then be fed through into the LearningSpace, providing a richer and broader set of resources. The OU has also adopted the open source Virtual Learning Environment (VLE) Moodle (www.moodle.org) to deliver content to students and to provide innovations in VLE which are fed back to the worldwide community.

6.2 Hybrid course development

We have recognised that the traditional course development model cannot be expected to produce timely and relevant material, and have therefore embarked on a novel course development model. The new course consists of three large blocks of material, each of which is introduced and concluded with high quality printed course units representing perhaps one third of the total learning material. These units will contain material relatively immune to change such as basic concepts and discussions of social importance. Since these units will remain unchanged for a number of years, they will be generated using the traditional production methods and presented as glossy, high-value booklets.

The remainder of the units will be delivered online, with each unit being made up from short 'articles' much like a magazine. Articles can be tagged and commented by students, although their contents cannot be changed. Web delivery allows for faster, cheaper, more flexible development and presentation of timely material. Short articles are easier to replace as they become outdated, or prove to be unpopular with students or unduly difficult,

ensuring that the course remains relevant for longer. The articles also allow us to widen the course team to almost anyone—not just the team developing the new course, but fellow academics both inside our own department and in the wider university. We also intend to present articles written by researchers in the field from outside the OU, including practitioners.

7 Summary

At the OU we consider security to be a fundamental computing issue, so much so that if a student only completes an introductory course in computer science they will have a comprehension of its importance, scope, and applicability to their lives. Those students who choose to continue studying computing will encounter many different aspects of security throughout the curriculum, allowing them to comprehend its complexity and diversity.

Security is a high value skill in a globalized market. Software and hardware businesses will have an increasing need for in house security skills at all levels in years to come, as low level skills such as programming and customer support are outsourced. The rate of change continues to increase and traditional university teaching methods cannot be expected to keep pace. Consequently we are increasingly utilizing a practitioner-led course development model to produce relevant, timely teaching, using real-world examples for assessment.

By sharing our experience, course content and tools through open content and open source initiatives, the Open University is enabling educators and professionals to collaborate in the development and deployment of novel teaching and technologies such as security. Our ultimate ambition should be to create a world class free resource accessible to anyone.

References

[1] www.swebok.org [Accessed 28 November 2007]

[2] www.acm.org/education/curricula.html [Accessed 2007-11-28]

[3] B. Bogolea and K. Wijekumar, “Information security curriculum creation: a case study,” In *Proceedings of the 1st Annual Conference on information Security Curriculum Development* (Kennesaw, Georgia, October 08–08, 2004). InfoSecCD’04. ACM, New York, NY, 59–65. DOI=http://doi.acm.org/10.1145/1059524.1059537

[4] http://www.foresight.gov.uk/HORIZON_SCANNING_CENTRE/Reports/S-TClusters/S_T_clusters__security-doc.pdf [Accessed 2007-11-28]

[5] H.J.C. Ellis Software engineering at a distance. Proceedings of the 1998 International Conference on Software Engineering, 23–24 (1998).

[6] M. Woodman, R. Griffiths, M. Macgregor and S. Holland, OU LearningWorks: a customized programming environment for Smalltalk modules. Proceedings of the 1999 International Conference on Software Engineering, 638–641 (1999).

[7] H. Sharp and P. Hall An interactive multimedia software house simulation forpostgraduate software engineers. Proceedings of the 2000 International Conference on Software Engineering, 688–691 (2000).

[8] B. Quinn, L. Barroca, B. Nuseibeh, J. Fernandez-Ramil, L. Rapanotti, P. Thomas, and M. Wermelinger Learning Software Engineering at a Distance. *IEEE Software* vol. 23, no. 6, pp. 36–43 (2006).

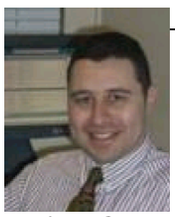
[9] http://www.hefce.ac.uk/learning/nss/ [Accessed 2007-11-28]

Mike RICHARDS

Mike RICHARDS is a Lecturer in Computing at The Open University, UK. He was awarded the BSc in Geology from the University College of Wales, Aberystwyth, UK, in 1988 the Master of Science in Computer Science from the University of Wales in 1990. In 1996 he joined the Open University to help launch the large scale Internet teaching programme for Computer Science. His research interests include privacy and security in ubiquitous computing. His teaching subjects include introductory computing, artificial intelligence and information security.

Blaine PRICE

Blaine PRICE is a Lecturer in Computing at The Open University. He has undergraduate degrees in both Mathematics and Computing & Information Science from Queen’s University at Kingston, Canada. He was awarded the Master of Science in Computer Science from the University of Toronto in 1991 when he joined the Open University. He is largely responsible for the Open University’s early work in large scale teaching via the Internet. His research areas include security and privacy in ubiquitous computing. He chairs the MSc in Computing and conducts both research and teaching in the areas of forensic computing and IT law.



Bashar NUSEIBEH

Bashar NUSEIBEH is Professor and Director of Research in Computing at The Open University, and a Visiting Professor at Imperial College London and the National Institute of Informatics, Japan. His research interests are in software requirements engineering and design, particularly applied to the development of dependable, mission-critical systems. Professor Nuseibeh is Editor-in-Chief of the Automated Software Engineering Journal, Chair of IFIP Working Group 2.9 on Requirements Engineering, and Chair of the Steering Committee of the International Conference on Software Engineering. He received a number of research and service awards, and is an Automated Software Engineering Fellow, a Fellow of the British Computer Society and the Institution of Engineering and Technology, and is a Chartered Engineer.